ABSTRACT OF THE DISCLOSURE

A client-server authentication method for use where a server process has access to a repository storing cipher-protected client passwords. The method includes applying the same cipher function to the client's copy of its password as was previously applied to generate the stored cipher-protected client passwords. This ensures that both the client and server have access to an equivalent cipher-protected client password - providing a shared secret for driving a mutual challenge-response authentication protocol without having to convert the password into cleartext at the server. The invention can be implemented without significant additional software infrastructure in a UNIX environment. Client passwords are typically stored in the UNIX password repository under the protection of the crypt() function applied to the combination of the password and a random number (a 'salt'). By sending the salt to the client system together with the server's initial challenge of the authentication protocol, a process at the client is able to apply the crypt() function to the client password with the same salt such that the client and server have a shared secret for use as, or to generate, a common session key for the authentication.